REMARKS

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1-9, 12, 15-17, 19-31, 34-36, 38, 39 and 41 are currently pending
- Claims 1, 20 and 39 are amended herein

[0003] Support for the amendments to claims 1, 20 and 39 is found in the specification at least at page 15, lines 1-8. Specifically, independent claims 1, 20 and 29 have been amended to clarify that assembling the messages into a message sequence is based upon: a specified participant; a specified time frame; a transaction nature; **and** the role played by the specified participant. The aforementioned clarification distinguishing over the previous claim scope wherein the combining was based upon simply "one or more of" the aforementioned elements instead of the presently claimed combination.

Claims 1, 20 and 39 Comply With § 112 2nd Paragraph

[0004] Claims 1, 20 and 39 stand rejected under 35 U.S.C. § 112, ¶ 2, as allegedly being indefinite. Applicant respectfully traverses this rejection.

[0005] Nevertheless, for the sole purpose of expediting prosecution and without acquiescing in the propriety of the Office's rejections, Applicant herein amends claims 1, 20 and 39 as shown above. Applicant respectfully submits that these amendments render the § 112, ¶ 2 rejections moot.

Cited Documents

[0006] The following documents have been applied to reject one or more claims of the Application:

- Clifton: Clifton et al., "Developing Custom Intrusion Detection Filters Using Data Mining", IEEE, 2000, pp 440-443
- Denning: Denning, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Vol. SE-13, No 2, February 1987, pp 222-232
- Vijaykumar: Vijaykumar, U.S. Patent No. 5,745,896
- Kay: Kay, U.S. Patent Application Publication No. 20040099125
- Julisch: Julisch, "Mining Alarm Clusters to Improve Alarm Handling Efficiency", IEEE, 2001, 10 pages
- Cuppens: Cuppens, "Managing Alerts in a Multi-Intrusion Detection Environment", IEEE, 2001, 10 pages
- Hofmeyr: Hofmeyr et al., "Intrusion Detection using Sequences of Systems Calls", August 18, 1998, pp 1-25
- Na: Na et al., U.S. Patent Application Publication No. 20030149679
- Greifeneder: Greifeneder et al., U.S. Patent Application Publication No. 20040243349

Claims 1-4, 8-9, 12, 15-17, 19, 21-23, 27-31, 34-36, 38 and 41 Are Non-Obvious Over Clifton, Cuppens, Denning, Vijaykumar, Kay and in further view of Julisch

[0007] Claims 1-4, 8-9, 12, 15-17, 19, 21-23, 27-31, 34-36, 38 and 41 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Clifton, Cuppens, Denning, Vijaykumar, Kay and in further view of Julisch. Applicant respectfully traverses the rejection.

Independent Claim 1

[0008] Applicant submits that the Office has not made a prima facie showing that independent claim 1 as amended is obvious in view of the combination of Clifton, Cuppens, Denning, Vijaykumar, Kay and in further view of Julisch. Applicant submits that the combination of Clifton, Cuppens, Denning, Vijaykumar, Kay and in further view of Julisch does not teach or suggest the following features of this claim, as amended (with emphasis added):

> **1. (Currently Amended)** A method for investigating messages passed in a message-passing environment, the method comprising:
>
> collecting message traces from at least one participant in the message-passing environment, wherein each message trace is a series of messages originating from or sent to the at least one participant, ordered by time, wherein each message has a first piece describing transfer of information and a second piece describing an operation being performed in the message;

converting identifying information pertaining to the at least one participant into an indication of a role played by the at least one participant in the message-passing environment;

assembling the messages into at least one message sequence, wherein assembling the message comprises combining multiple message traces into the at least one message sequence, each message trace pertaining to one or more messages transmitted by, or received at, a participant, wherein [[the]] combining multiple message traces is based on:

a specified participant;

a specified time frame;

a transaction nature; and

the role played by the specified participant;

analyzing the at least one message sequence from the message-passing environment to extract information regarding the at least one participant in the message-passing environment, wherein the analyzing comprises comparing at least one message sequence with a reference message sequence, the reference message sequence comprises at least one of a sequence that reflects an error-free operation in the message passing environment and a sequence that reflects known failure conditions in the message passing environment;

performing cluster analysis to group the at least one message sequence into at least one cluster, wherein the cluster analysis includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix, at least one cluster includes the reference sequence;

sorting into a ranked order at least two clusters based on a number of members associated with each cluster, the sorting prioritized from least members to most members associated each of the at least two clusters; and

outputting [[the]] information into a table format based on the sorting into a ranked order, each cluster represented in the table format is linked to information regarding an associated message sequence.

[0009] Claim 1 recites in part, that "combining multiple message traces is based on: a specified participant; a specified time frame; a transaction nature; and the role played by the specified participant." The Office cites Clifton, [Sequential Association Mining] as teaching this element. (Office Action, page 5.) The Office states:

wherein assembling includes combining multiple message traces (e.g., log(event, fromIP, toIP, time) into the at least one message sequence (e.g., 2,3,4, and 5-events), each message trace pertaining to one or more messages transmitted by, or received at, a participant (e.g., it is understood that a machine generates an attack, identified as an alarm. Log(event, FromIP, ToIP) is a message received, transmitted at a machine) , wherein the combining is based on one or more of, a specified participant, a specified time frame (e.g., one-minute window), a transaction nature ([Straightforward Count] e.g. Syn Flood, ident, print), and the role played by the at least one participant (e.g., FTP user);

[0010] Applicant respectfully traverses the Office's rejection, but in an attempt to more speedily advance prosecution, Applicant has amended claim 1. Applicant amends herein claim 1 to clarify that ""combining multiple message traces is based on: a specified participant; a specified time frame; a transaction nature; and the role played by the specified participant." As pointed out by the Examiner, Clifton does make reference to a specified time frame and a transaction nature. Clifton fails to teach or suggest that combining multiple message traces is based upon a specified participant. As such,

Clifton also fails to teach combining multiple message traces based on "the role played by the **specified** participant."

[0011] Consequently, the combination of cited art does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Dependent Claims 2-9, 12, 15-17 and 19

[0012] Claims 2-9, 12, 15-17 and 19 ultimately depend from independent claim 1. As discussed above, claim 1 is allowable over the cited documents. Therefore, claims 2-9, 12, 15-17 and 19 are also allowable over the cited documents of record for at least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Independent claim 20 and dependent claims 21-31, 34-36, 38 and 41

[0013] Applicant respectfully contends that the arguments set forth above with respect to independent claim 1, as amended, applies with equal weight here and the cited art does not teach or suggest all of the claimed elements and features of independent claim 20. Accordingly, Applicant respectfully asks the Examiner to withdraw the rejections of this claim. Further, dependent claims 21-31, 34-36, 38 and 41 are allowable for at least the same reasons that independent claim 20 is allowable. Applicant respectfully requests that the Examiner withdraw the rejection of dependent claims 21-31, 34-36, 38 and 41.

Independent claim 39

[0014] Applicant respectfully contends that the arguments set forth above with respect to independent claim 1, as amended, applies with equal weight here and the cited art does not teach or suggest all of the claimed elements and features of independent claim 39. Accordingly, Applicant respectfully asks the Examiner to withdraw the rejections of this claim.

Conclusion

[0015] Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned representative for the Applicant before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Jason F. Lindh Reg. No. 59, 090/ Dated: 2009-08-06
Jason F. Lindh (jason@leehayes.com; 509-944-4715)
Registration No. 59090